Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	
	)	
	)	

COMMENTS OF THE STATE PRIVACY AND SECURITY COALITION

Jim Halpert
Anne Kierig
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

March 6, 2017

I. INTRODUCTION

The State Privacy and Security Coalition, Inc., a coalition of 25 leading communications, technology, retail, and media companies and six trade associations that follows closely all the state data privacy and breach legislation , respectfully submits these brief comments in support of the petitions for reconsideration of the Broadband Privacy Order ("Final Rules").[1]

II. THE BREACH NOTIFICATION TIMELINE IS FAR SHORTER THAN UNDER ANY STATE BREACH NOTICE LAW

The Final Rule's breach notice deadline is confusingly out of kilter with both state and FTC law. None of the 47 state breach notification laws requires notice to a consumer protection agency or law enforcement within 7 days[2], or consumers within 30 days of determination of a breach. The shortest deadline for consumer notice is in Florida, where notice must presumptively be provided within 30 calendar days but may be extended a further 15 days with a routine request to the State AG's Office. Most states have no deadline for consumer notice. The states that do have a deadline for notice have deadlines of 45 days or longer.[3]

The FTC noted in bi-partisan comments in the Broadband Privacy proceeding that the Proposed Rule's 10-day notice requirement to consumers (seven days to law enforcement) is too short and may not allow companies sufficient time to conduct an investigation.[4] Companies need adequate time to do a thorough and accurate investigation before notifying affected parties

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) (Order).

[2] Vermont, an outlier, requires AG notice within 14 days unless a business has certified that it has an information security and incident response plan. VT. Stat. tit. 9 § 2435(b)(3)(B)(i). The next shortest deadline is in Florida, which requires AG notice within 30 days. Fla. Stat. §501.171(3)(a).

[3] *See e.g.*, Wis. Stat. § 134.98, "[A]n entity shall provide the notice required under sub. (2) within a reasonable time, not to exceed 45 days after the entity learns of the acquisition of personal information."

[4] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, pp. 32-33.

about a breach; complex breaches take time to investigate. It does not help anyone if businesses notify consumers prematurely with incorrect information.

In this respect, as well, the Final Rule departs sharply and arbitrarily from the FTC and state privacy and security frameworks.

III. THE SECURITY REQUIREMENTS IN THE RULES DIFFER FROM SENSITIVE DATA DEFINITIONS UNDER STATE, AS WELL AS FTC, LAW

As the petitioners observe, the Final Rules adopt an asymmetrical definition of sensitive data that would create consumer confusion and hinder innovation. This definition differs significantly not only from the FTC privacy framework, but also from all the state privacy and security statutes. No state privacy breach law or data security law treats web browsing data or app usage data held by ISPs or others as sensitive data. Nor does any state law require notification about breaches of these data.

The 47 state data security and data breach notice laws apply to the name of a state resident plus a sensitive data element. The sensitive data elements vary by state, but include social security number, government identification number, financial account number in combination with a code to access a financial account, and in some states medical information, health insurance claim information or user name and password for an online account.[5] States have considered and uniformly rejected proposals to require notification of all personally identifiable information,[6] of websites visited by state residents,[7] which are included in the Final Rules' definition of "sensitive customer information."[8]

[5] *See, e.g.*, Cal. Civ. Code § 1798.82(h) (defining "personal information").
[6] Nevada AB 0179 (2015).
[7] Illinois SB 1833 (2015).
[8] *See, e.g.*, Kan. Stat. § 50-7a01(g).

Furthermore, the Final Rules require broadband providers to similarly secure *all information* that is "linked or linkable" to a customer.[9] This is contrary to the FTC "Start with Security Guide for Business", which directs businesses to focus their security programs on "sensitive data" ,[10] and to all the state data security laws.[11]

The broad scope of the FCC Rule would lead to over-notification of breaches that do not pose a harm of identity theft or fraud to consumers. For example, if IP addresses were to be acquired in a breach, the FCC Rule would require notice. An IP address alone, however, likely cannot be used to cause harm. Moreover, there is nothing a consumer can do to address the acquisition of an IP address. The Rule would be more effective if it were aligned with state laws pertaining to the security of sensitive data definitions.

IV. CONCLUSION

For all these reasons, we urge the Commission to grant the petitions for reconsideration to align the Rules with the FTC's privacy, data security and breach notice standards that apply across the Internet ecosystem.

Respectfully submitted,

/s/

Jim Halpert
Anne Kierig
Counsel to the State Privacy and Security Coalition, Inc.
DLA Piper LLP (US)
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

[9] Order, ¶ 89.
[10] *Start With Security, A Guideline for Business*, Federal Trade Commission Guidelines, p. 6, found at the following link: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[11] *See, e.g.,* California Business & Professions Code 1798.81.5(d).